

ABSTRACT

A monitor for information technology resources improved by introducing typicality filters to analyze potential event indicators such as alerts. A typicality filter keeps a time-dependent history of the frequency of occurrence of an associated event, wherein time is segmented into monitoring periods. At the end of each monitoring period, a present count of occurrences of the event is determined, and compared with the numbers of occurrences of that event in a subset of monitoring periods read from the history. If the present count exceeds the number of occurrences of the event in a predetermined proportion of the subset of historical monitoring periods, a first action is invoked; otherwise, a second action is invoked.